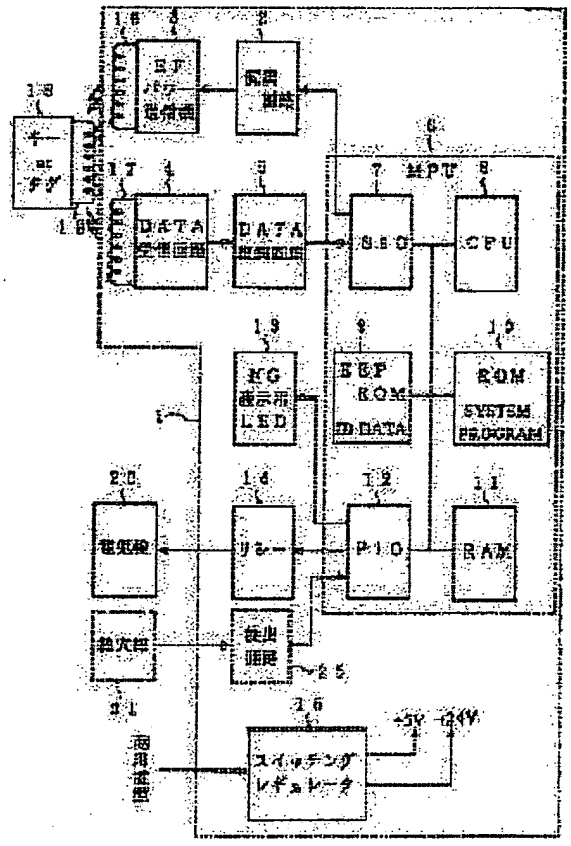
3119112

LOCKING DEVICE FOR VENDING MACHINE

Publication number: JP10110563 (A) IDS未
Publication date: 1998-04-28
Inventor(s): SASAKI KAZUO; HIRANO MASAMI +
Applicant(s): UNITEC KK; TAKIGEN MFG CO +
Classification:
- international: ***E05B49/00; E05B65/02; G01S13/75; G01S13/76; G01S13/79; G07F9/00;*** **E05B49/00; E05B65/02; G01S13/00; G07F9/00;** (IPC1-7): E05B49/00; E05B65/02; G01S13/75; G01S13/76; G01S13/79
- European:
Application number: JP19960284648 19961007
Priority number(s): JP19960284648 19961007

Abstract of **JP 10110563 (A)**

PROBLEM TO BE SOLVED: To prevent the breakage of a lock, and to minimize the damage even when a lock hole is broken. SOLUTION: A vending machine is provided with a dummy key hole. When a key is inserted in the key hole, a reader 1 of the vending machine transmits the RF power signal. A transponder 18 of the key is operated by receiving the RF power signal, and the ID data (the system discrimination ID data, the master key group ID data, and the key ID data) stored in an EEPROM are transmitted according to the data requesting command from the reader 1. The reader 1 receives the ID data, and compares the received data with the ID data preset in an EEPROM 9, and when all the data agree, a relay 14 is driven to open an electric lock 20. Because the key hole is simply a dummy to detect the unlocking, the damage can be minimized even when the lock is broken.



Data supplied from the *espacenet* database — Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－110563

(43)公開日　平成10年(1998)４月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｊ
65/02		65/02	Ｃ
Ｇ０１Ｓ　13/75		Ｇ０１Ｓ　13/80	
13/76			
13/79			

審査請求　未請求　請求項の数９　ＦＤ　（全 15 頁）

(21)出願番号　特願平8－284648

(22)出願日　平成８年(1996)10月７日

(71)出願人　391030538
ユニテック株式会社
東京都大田区中央２丁目25番６号

(71)出願人　000108708
タキゲン製造株式会社
東京都品川区西五反田１丁目24番４号

(72)発明者　佐々木　和夫
東京都大田区中央２丁目25番６号　ユニテック株式会社内

(72)発明者　平野　正己
東京都大田区中央２丁目25番６号　ユニテック株式会社内

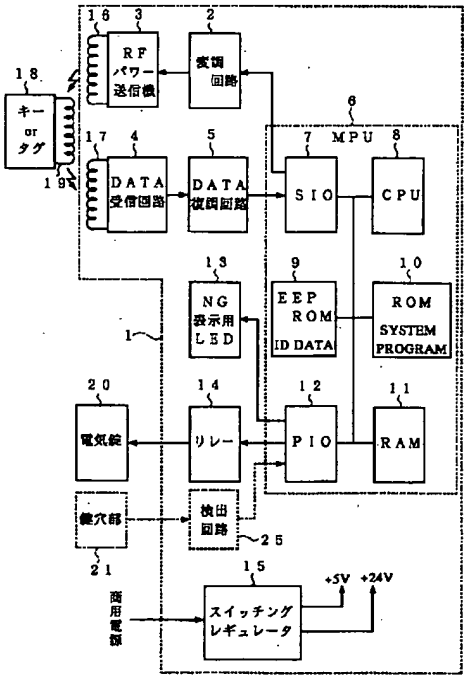
(74)代理人　弁理士　鹿嶋　英實

(54)【発明の名称】　自動販売機の鍵装置

(57)【要約】

【課題】　錠の破壊を防止することができ、また、仮に錠穴が破壊されても、被害規模を最小にすることができる自動販売機の鍵装置を提供する。

【解決手段】　上記自動販売機には、ダミーの鍵穴が設けられている。自動販売機のリーダ１は、鍵穴に鍵が挿入されると、ＲＦパワー信号を送信する。鍵のトランスポンダ１８は、上記ＲＦパワー信号を受信することで作動し、ＥＥＰＲＯＭ２４に記憶されているＩＤデータ（システム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータ）を、リーダ１からのデータ要求コマンドに応じて送信する。リーダ１は、上記ＩＤデータを受信し、ＥＥＰＲＯＭ９に予め設定されているＩＤデータと比較し、全てが一致すると、リレー１４を駆動して電気錠２０を開く。上記鍵穴は、単に、開錠されることを検知するためのダミーであるので、仮に破壊されたとしても、最小の被害で済む。



1

【特許請求の範囲】

【請求項１】　外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第１の記憶手段および電力が印加されると前記第１の記憶手段に記憶されている応答装置識別データを送信する第１の送信手段を備える応答装置と、

前記高周波磁界を発生する高周波発生手段、前記第１の送信手段から送信された応答装置識別データを受信する第１の受信手段、自動販売機の扉を施錠する電気錠、前記自動販売機の扉を開けることを許可する応答装置を特定する応答装置識別データを記憶する第２の記憶手段、前記第１の受信手段によって受信された応答装置識別データと前記第２の記憶手段に記憶されている応答装置識別データとが一致した場合、前記電気錠を開ける第１の制御手段を備え、前記自動販売機に設けられる読み取り装置とを具備することを特徴とする自動販売機の鍵装置。

【請求項２】　前記読み取り装置は、前記第１受信手段によって受信された応答装置識別データと前記第２の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備することを特徴とする請求項１記載の自動販売機の鍵装置。

【請求項３】　前記応答装置は、鍵形状部分を有し、前記自動販売機は、前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えることを特徴とする請求項１記載の自動販売機の鍵装置。

【請求項４】　前記読み取り装置は、前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知されると、前記高周波発生手段によって高周波磁界を発生することを特徴とする請求項３記載の自動販売機の鍵装置。

【請求項５】　前記応答装置は、カード形状であり、前記読み取り装置は、前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生することを特徴とする請求項１記載の自動販売機の鍵装置。

【請求項６】　前記応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受することを特徴とする請求項１ないし５記載の自動販売機の鍵装置。

【請求項７】　前記応答装置は、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第２の制御手段を備え、

前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記

2

マスタ・キー・グループ識別データおよび前記応答装置識別データを授受することを特徴とする請求項１ないし５記載の自動販売機の鍵装置。

【請求項８】　前記読み取り装置は、前記応答装置に対してデータを送信する第２の送信手段と、前記制御手段によって前記電気錠が開けられると、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第２の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第１の更新手段とを備え、前記第２の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、

前記応答装置は、前記読み取り装置が送信するデータを受信する第２の受信手段と、前記第１の記憶手段に記憶されている応答装置識別データを、前記第２の受信手段によって受信した前記新たな応答装置識別データで書き換える第２の更新手段とを備えることを特徴とする請求項１ないし７記載の自動販売機の鍵装置。

【請求項９】　前記応答装置識別データおよびマスタ・キー・グループ識別データは、外部設定装置により無線通信により書換可能であることを特徴とする請求項１ないし８記載の自動販売機の鍵装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、商品の無人販売に用いられる自動販売機に用いて好適な自動販売機の鍵装置に関する。

【０００２】

【従来の技術】従来より、商品の無人販売に用いられる自動販売機においては、筐体に設けられている鍵穴に、所定の鍵を差し込んで錠を外し、自動販売機を開けることで、商品の補充・交換、あるいは代金の回収が行われている。

【０００３】

【発明が解決しようとする課題】ところで、従来の自動販売機では、鍵穴が見えるため、錠の位置が容易に判別できる。このため、筐体に設けられている錠が破壊され、内部の代金や商品が盗難されるという問題があった。 特に、現金盗難の被害額より、錠修理に要する額の方が大きいので、錠の破壊を防止する必要がある。

【０００４】そこで本発明は、錠の破壊を防止することができ、また、仮に錠穴が破壊されても、被害規模を最小にすることができる自動販売機の鍵装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的達成のため、請求項１記載の発明による自動販売機の鍵装置は、外部の高周波磁界を各部を駆動するための電力とする装置であって、当該装置を識別するための応答装置識別データを記憶する第１の記憶手段および電力が印加されると前記

第１の記憶手段に記憶されている応答装置識別データを送信する第１の送信手段を備える応答装置と、前記高周波磁界を発生する高周波発生手段、前記第１の送信手段から送信された応答装置識別データを受信する第１の受信手段、自動販売機の扉を施錠する電気錠、前記自動販売機の扉を開けることを許可する応答装置を特定する応答装置識別データを記憶する第２の記憶手段、前記第１の受信手段によって受信された応答装置識別データと前記第２の記憶手段に記憶されている応答装置識別データとが一致した場合、前記電気錠を開ける第１の制御手段を備え、前記自動販売機に設けられる読み取り装置とを具備することを特徴とする。

【０００６】また、好ましい態様として、前記読み取り装置は、例えば請求項２記載のように、前記第１受信手段によって受信された応答装置識別データと前記第２の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告を発する警告手段を具備するようにしてもよい。

【０００７】また、好ましい態様として、前記応答装置は、例えば請求項３記載のように、鍵形状部分を有し、前記自動販売機は、前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えるようにしてもよい。

【０００８】また、好ましい態様として、前記読み取り装置は、例えば請求項４記載のように、前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知されると、前記高周波発生手段によって高周波磁界を発生するようにしてもよい。

【０００９】また、好ましい態様として、前記応答装置は、例えば請求項５記載のように、カード形状であり、前記読み取り装置は、前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生するようにしてもよい。

【００１０】また、好ましい態様として、前記応答装置および前記読み取り装置は、例えば請求項６記載のように、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしてもよい。

【００１１】また、好ましい態様として、前記応答装置は、例えば請求項７記載のように、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第２の制御手段を備え、前記応答装置および前記読み取り装置は、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受するようにしてもよい。

【００１２】また、好ましい態様として、前記読み取り装置は、例えば請求項８記載のように、前記応答装置に対してデータを送信する第２の送信手段と、前記制御手段によって前記電気錠が開けられると、新たな応答装置識別データを生成する応答装置識別データ生成手段と、前記第２の記憶手段に記憶されている応答装置識別データを、前記応答装置識別データ生成手段によって生成された新たな応答装置識別データで書き換える第１の更新手段とを備え、前記第２の送信手段によって前記新たな応答装置識別データを前記応答装置に対して送信し、前記応答装置は、前記読み取り装置が送信するデータを受信する第２の受信手段と、前記第１の記憶手段に記憶されている応答装置識別データを、前記第２の受信手段によって受信した前記新たな応答装置識別データで書き換える第２の更新手段とを備えるようにしてもよい。

【００１３】また、好ましい態様として、前記応答装置識別データおよびマスタ・キー・グループ識別データは、例えば請求項９記載のように、外部設定装置により無線通信により書換可能であってもよい。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を、自動販売機に適用した一実施例として、図面を参照して説明する。

Ａ．実施例の構成

Ａ－１．自動販売機に内蔵されるリーダおよび鍵（トランスポンダ）の構成

図１は本発明の実施例による自動販売機に内蔵されるリーダおよびトランスポンダが内蔵された、自動販売機の錠を開錠するための鍵の構成を示すブロック図である。また、図４は、上記トランスポンダのより詳細な構成例を示すブロック図である。図において、リーダ１は、自動販売機に内蔵されており、変調回路２、ＲＦパワー送信機３、ＤＡＴＡ受信回路４、ＤＡＴＡ復調回路５、ＭＰＵ６、ＮＧ表示用ＬＥＤ１３、リレー１４、スイッチングレギュレータ１５等から構成されている。以下、各部について説明する。

【００１５】変調回路２は、所定の信号を１２５ＫＨｚでＦＳＫ変調し、ＲＦパワー送信機３に供給する。ＲＦパワー送信機３は、上記変調信号をアンテナ１６より送信する。上記信号としては、鍵に内蔵されている後述するトランスポンダ１８を作動させるためのＲＦパワーや、トランスポンダ１８に対して各種ＩＤ送信を要求するためのコマンドがある。次に、ＤＡＴＡ受信回路４は、後述するトランスポンダ１８から送信される、６２．５ＫＨｚでＰＳＫ変調された信号をアンテナ１７で受信し、ＤＡＴＡ復調回路５に供給する。ＤＡＴＡ復調回路５は、受信信号を復調し、データ（各種ＩＤ）を取り出し、ＭＰＵ６のＳＩＯ（シリアル入出力インターフェース）７へ供給する。

【００１６】ＭＰＵ６は、上記ＳＩＯ７、ＣＰＵ（中央処理装置）８、ＥＥＰＲＯＭ９、ＲＯＭ（リードオンリ

メモリ）１０、ＲＡＭ（ランダムアクセスメモリ）１１およびＰＩＯ（パラレル入出力インターフェース）１２から構成されている。ＳＩＯ７は、上記ＤＡＴＡ復調回路５からのデータをＣＰＵ８に供給する。ＣＰＵ８は、ＲＯＭ１０に格納されているプログラムを実行し、各種コマンドの送信、トランスポンダ１８からの各種データの受信、トランスポンダ１８の認証、後述するリレー駆動による電気錠２０の開錠等の制御を行う。ＥＥＰＲＯＭ９には、自動販売機に内蔵された当該リーダ１に対応するトランスポンダ１８を識別するための各種ＩＤデータが記憶されている。言い換えると、本リーダ１は、該ＥＥＰＲＯＭ９に記憶されているＩＤデータに一致するＩＤデータを送信するトランスポンダ１８が近接した場合にのみ、電気錠２０を開錠するようになっている。

【００１７】また、ＲＯＭ１０には、上述したように、ＣＰＵ８によって実行されるプログラムが格納されている。ＲＡＭ１１は、上記ＣＰＵ８の制御に伴って生成されるデータが格納されたり、ワーキングエリアとして用いられる。ＰＩＯ１２は、ＣＰＵ８の制御の下、ＣＰＵ８から供給される表示データをＮＧ表示用ＬＥＤ１３に供給するとともに、ＣＰＵ８から供給されるリレー駆動用データをリレー１４に供給する。ＮＧ表示用ＬＥＤ１３は、トランスポンダ１８から送信されるＩＤデータが上記ＥＥＰＲＯＭ９に格納されているＩＤデータと不一致である場合、すなわち、適合しないトランスポンダで開錠されようとした場合に、点灯される表示部である。次に、リレー１４は、上記リレー駆動用データが供給されると、電気錠２０を作動させて開錠する。スイッチングレギュレータ１５は、図示しない商用電源を整流し、直流電圧として、＋５Ｖ、＋２４Ｖを発生し、上述した各部へ電源として供給する。

【００１８】また、鍵穴２１は、例えば、自動販売機の前面に設けられている。但し、本実施例では、以下において、鍵穴２１を設ける場合と、鍵穴２１を設けない場合とについて説明している。また、鍵穴２１は、いわゆるダミーであり、操作しやすい場所であれば、特に、電気錠２０が配設されている場所を避ければ、どこに設けてもよい。これは、仮に、鍵穴２１が破壊されても、電気錠自体を破壊することができないようにするためである。検出回路２５は、上記鍵穴２１に鍵が挿入されたことを検出し、ＰＩＯ１２を介してＣＰＵ８に知らせる。このように、鍵穴２１を設けた場合には、ＣＰＵ８は、ＲＦパワー送信機３からＲＦパワー信号を送信する。

【００１９】Ａ－２．自動販売機の外観構成

図２および図３は、上述したリーダが内蔵された自動販売機の外観構成を示す斜視図である。本実施例では、トランスポンダを内蔵する鍵として、カード形状のものと、通常の鍵形状のものの２つの構成例を採用している。したがって、トランスポンダ１８にカード形状のものを採用した場合には、図２に示すように、自動販売機

には、鍵穴はなく、トランスポンダ１８からのＩＤ認証によって開錠される電気錠のみが設けられている。また、トランスポンダ１８に通常の鍵形状のものを採用した場合には、図３に示すように、自動販売機には、上記トランスポンダ１８からのＩＤ認証によって開錠される電気錠とともに、該鍵が差し込まれる鍵穴２１が設けられている。この場合、鍵穴２１は、上述したように、鍵を挿入することで、実際に機械式の錠を開けるためのものではなく、トランスポンダ１８が内蔵された鍵が挿入されたことを検知することで、メンテナンス等のために、開錠しようとしていることを認識するために用いられるものである。

【００２０】本実施例では、鍵に内蔵されているトランスポンダ１８は、自動販売機に内蔵されたリーダ１から送信されるＲＦパワー信号を電源として作動するようになっている。したがって、鍵にカード形状のものを採用した場合には、いつ鍵がリーダ１の通信範囲に入ったかを知ることができないため、常時あるいは所定時間間隔で、ＲＦパワー信号を送信しなければならない。これに対して、自動販売機に鍵穴を設けた場合には、リーダ１は、鍵が自動販売機の鍵穴に挿入された時点で、ＲＦパワー信号を送信し、トランスポンダ１８を作動させればよく、省電力化に効果がある。また、上記鍵穴が実際に開閉するための電気錠のものではないので、鍵穴は、必ずしも電気錠部分に設ける必要はない。したがって、鍵穴をこじ開けることにより、不正に開錠しようとしても、開錠することはできず、また、仮に鍵穴が破壊されたとしても、鍵穴修理に要する金額が小さいので、容易に修理できる。

【００２１】Ａ－３．トランスポンダの構成

図４（ａ）、（ｂ）は、上述したトランスポンダ１８の構成例を示すブロック図である。図４（ａ）に示すトランスポンダ１８は、アンテナ１９、送受信回路２２、ＣＰＵ２３、ＥＥＰＲＯＭ２４から構成されている。アンテナ１９は、上述したリーダ１から送信されるＲＦパワー信号や変調信号を受信し、送受信回路２２に供給する。送受信回路２２は、図示しない整流回路を備えており、受信したＲＦパワー信号を整流して所定の直流電圧を取り出し、ＣＰＵ２３およびＥＥＰＲＯＭ２４に電源として供給するとともに、受信信号を復調し、リーダ１から送信される各種コマンドを取り出してＣＰＵ２３に供給する。

【００２２】ＣＰＵ２３は、プログラムを内蔵するＲＯＭやワークエリアとしてのＲＡＭ等を内蔵しており（図示略）、ＲＦパワー信号により作動し、リーダ１から送信される各種コマンドを解釈し、受信したコマンドに応じて、ＥＥＰＲＯＭ２４に予め格納されている各種ＩＤデータを読み出し、送受信回路２２によって変調してアンテナ１９から送信する。ＥＥＰＲＯＭ２４には、上述したように、予め各種ＩＤデータが記憶されており、該

各種ＩＤデータは、ＣＰＵ２３によって適宜読み出される。このように、図４（ａ）に示すトランスポンダ１８を採用した場合には、トランスポンダ１８は、リーダ１からのＩＤデータ要求コマンドに応じて、対応するＩＤデータを送信する。

【００２３】ここで、図５は、上記リーダ１と上記トランスポンダ１８とで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット、データ（１２ビット）、パリティビット、ストップビットから構成されており、１キャラクタ単位で、データ部分で各種ＩＤデータを送信し、その後にエラーチェック用のデータを同一フォーマットで１キャラクタ送信する。この場合、トランスポンダ１８は、図６に示すように、リーダ１からの要求に応じて、システム識別ＩＤデータ、マスターキーグループＩＤデータおよび鍵ＩＤデータを送信するようになっている。すなわち、トランスポンダ１８は、リーダ１からＲＦパワーを受信すると、まず、自動的に、システム識別ＩＤデータを送信し、次いで、マスターキーグループＩＤ要求コマンドを受信すると、これに応じて、マスターキーグループＩＤデータを送信し、さらに、鍵ＩＤ要求コマンドを受信すると、これに応じて、鍵ＩＤデータを送信する。

【００２４】なお、システム識別ＩＤデータは、例えば、自動販売機のメーカ毎に設定され、該メーカを識別するためのＩＤデータであり、固定値となっている。また、マスター・キー・グループＩＤデータは、自動販売機の設置場所でグループ化し、該グループを識別するためのＩＤデータであり、変更可能となっている。さらに、鍵ＩＤデータは、トランスポンダ（鍵）１８を識別するためのＩＤデータであり、やはり変更可能となっている。リーダ１は、これらシステム識別ＩＤデータ、マスターキーグループＩＤデータおよび鍵ＩＤデータの全てが一致した場合にのみ、電気錠を開錠するようになっている。

【００２５】一方、図４（ｂ）に示すトランスポンダ１８は、アンテナ１９、送受信回路２６およびＥＥＰＲＯＭ２７から構成されている。アンテナ１９は、上述したリーダ１から送信されるＲＦパワー信号や変調信号を受信し、送受信回路２６に供給する。送受信回路２６は、図示しない整流回路を備えており、受信したＲＦパワー信号を整流して所定の直流電圧を取り出し、ＥＥＰＲＯＭ２７に電源として供給するとともに、ＥＥＰＲＯＭ２７から供給される各種ＩＤデータを変調し、アンテナ１９から送信する。ＥＥＰＲＯＭ２７には、上述したように、予め各種ＩＤデータが記憶されており、電源が供給されると、記憶されていた各種ＩＤデータを自動的に送受信回路２６に供給する。このように、図４（ｂ）に示すトランスポンダ１８を採用した場合には、トランスポンダ１８は、ＲＦパワー信号を受信した時点で、ＥＥＰＲＯＭ２７に予め記憶されている各種ＩＤデータを送信する。

【００２６】ここで、図７は、上記リーダと上記トランスポンダとで授受されるデータフォーマットを示す概念図である。図示するように、データは、スタートビット（８ビット）、システム識別ＩＤデータ（１６ビット）、マスターキーグループＩＤデータ（２４ビット）、鍵ＩＤデータ（２４ビット）、データＢＣＣ（１６ビット）、ストップビット（８ビット）の全１２８ビットから構成されている。この場合、トランスポンダ１８は、図８に示すように、ＲＦパワーを受信することで作動すると、自動的に、上記データフォーマットで、システム識別ＩＤデータ、マスターキーグループＩＤデータおよび鍵ＩＤデータを送信するようになっている。なお、システム識別ＩＤデータ、マスターキーグループＩＤデータおよび鍵ＩＤデータの目的およびその内容は、前述した通りである。

【００２７】Ｂ．実施例の動作

次に、上述した実施例による自動販売機に内蔵されたリーダ１および鍵に内蔵されたトランスポンダ１８の動作について説明する。なお、以下では、上述したリーダ、トランスポンダ、データフォーマットの組み合わせに応じて、以下のケースについて各々の動作を説明する。

①ＣＰＵ有り、ＩＤ更新機能有り
②ＣＰＵ有り、ＩＤ更新機能無し
③ＣＰＵ無し、ＩＤ更新機能有り
④ＣＰＵ無し、ＩＤ更新機能無し

また、以下では、ＣＰＵ有り、ＩＤ更新機能有り・無し、およびＣＰＵ無し、ＩＤ更新機能有り・無しにおけるＩＤデータ設定処理の動作についても説明する。

【００２８】Ｂ－１．開錠処理（①ＣＰＵ有り、ＩＤ更新機能有り）

まず、ＣＰＵ２３を備えるトランスポンダ（ＩＤ更新機能有り）１８を用いた場合における開錠処理について説明する。ここで、図９および図１０は、ＣＰＵ２３を備えるトランスポンダ（ＩＤ更新機能有り）１８における、リーダ１およびトランスポンダ１８での開錠処理の動作を説明するためのフローチャートである。

【００２９】まず、自動販売機のリーダ１では、図９に示すステップＳ１０で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップＳ１２で、ＲＦパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップＳ１４でデータを受信するまで、所定時間間隔で、ＲＦパワー信号の送信を繰り返す。

【００３０】これに対して、鍵のトランスポンダ１８は、上記ＲＦパワー信号を受信することで作動し、図１０に示すステップＳ４０で、ＥＥＰＲＯＭ２４からシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを読み込む。次に、ステップＳ４２で、図５に示すデータフォーマットで、システム識別

ＩＤデータを送信する。

【００３１】リーダ１では、ステップＳ１４で、上記システム識別ＩＤデータを受信し、ステップＳ１６で、自身のＥＥＰＲＯＭ９に予め設定されているシステム識別ＩＤデータと照合し、一致すれば、ステップＳ１８に進み、マスタ・キー・グループＩＤデータ要求コマンドを送信する。これに対して、鍵のトランスポンダ１８では、ステップＳ４４で、上記マスタ・キー・グループＩＤデータ要求コマンドを受信すると、ステップＳ４６で、ステップＳ４０で読み出したマスタ・キー・グループＩＤデータを図５に示すデータフォーマットで送信する。リーダ１では、ステップＳ２０で、上記マスタ・キー・グループＩＤデータを受信する。自動販売機のリーダ１では、上記ステップＳ１８，Ｓ２０、鍵のトランスポンダ１８では、上記ステップＳ４４，Ｓ４６を繰り返すことにより、鍵ＩＤデータ要求コマンドの送受信、および鍵ＩＤデータの送受信を行い、図５に示すデータフォーマットで鍵ＩＤデータを授受する。

【００３２】次に、自動販売機のリーダ１では、ステップＳ２２で、上記マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを、ＥＥＰＲＯＭ９に予め設定されているＩＤデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップＳ２４に進み、リレー１４を駆動し、電気錠２０を開く。そして、ステップＳ２６で、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を乱数によって生成し、ＥＥＰＲＯＭ９のＩＤデータを更新し、記憶する。次に、ステップＳ２８で、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を送信する。

【００３３】これに対して、鍵のトランスポンダ１８では、ステップＳ４８で、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を受信し、該新たなＩＤデータで、ＥＥＰＲＯＭ２４のＩＤデータを書き換え、更新する。

【００３４】さらに、自動販売機のリーダ１では、ステップＳ３０で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵またはカード）１８を識別するための鍵ＩＤデータ（個別かマスタか）を記録する。

【００３５】また、リーダ１において、ステップＳ１６で、トランスポンダ１８から送信されたシステム識別ＩＤが自身のものと一致しない場合、あるいは、ステップＳ２２で、トランスポンダ１８から送信されたマスタ・キー・グループＩＤデータあるいは鍵ＩＤデータが自身のものと一致しない場合には、ステップＳ３２で、防犯および警報システムを作動させる。

【００３６】Ｂ－２．開錠処理（②ＣＰＵ有り、ＩＤ更新機能無し）

次に、ＣＰＵ２３を備えるトランスポンダ（ＩＤ更新機能無し）１８を用いた場合における開錠処理について説明する。ここで、図１１および図１２は、ＣＰＵ２３を備えるトランスポンダ（ＩＤ更新機能無し）１８における、リーダ１およびトランスポンダ１８での開錠処理の動作を説明するためのフローチャートである。

【００３７】まず、リーダ１では、図１１に示すステップＳ６０で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップＳ６２で、ＲＦパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップＳ６４でデータを受信するまで、所定時間間隔で、ＲＦパワー信号の送信を繰り返す。

【００３８】これに対して、鍵のトランスポンダ１８は、上記ＲＦパワー信号を受信することで作動し、図１２に示すステップＳ８０で、ＥＥＰＲＯＭ２４からシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを読み込む。次に、ステップＳ８２で、図５に示すデータフォーマットで、システム識別ＩＤデータを送信する。

【００３９】リーダ１では、ステップＳ６４で、上記システム識別ＩＤデータを受信し、ステップＳ６６で、自身のＥＥＰＲＯＭ９に予め設定されているシステム識別ＩＤデータと照合し、一致すれば、ステップＳ６８に進み、マスタ・キー・グループＩＤデータ要求コマンドを送信する。

【００４０】これに対して、鍵のトランスポンダ１８では、ステップＳ８４で、上記マスタ・キー・グループＩＤデータ要求コマンドを受信すると、ステップＳ８６で、ステップＳ８０で読み出したマスタ・キー・グループＩＤデータを図５に示すデータフォーマットで送信する。リーダ１では、ステップＳ７０で、上記マスタ・キー・グループＩＤデータを受信する。そして、自動販売機のリーダ１では、上記ステップＳ６８，Ｓ７０、鍵のトランスポンダ１８では、上記ステップＳ８４，Ｓ８６を繰り返すことにより、鍵ＩＤデータ要求コマンドの送受信、および鍵ＩＤデータの送受信を行い、図５に示すデータフォーマットで鍵ＩＤデータを授受する。

【００４１】次に、自動販売機のリーダ１では、ステップＳ７２で、上記マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを、ＥＥＰＲＯＭ９に予め設定されているデータと照合することにより、一致するか否かを判断し、それぞれ一致すると、ステップＳ７４に進み、リレー１４を駆動し、電気錠２０を開く。さらに、自動販売機のリーダ１では、ステップＳ７６で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵またはカード）１８を識別するための鍵ＩＤデータ（個別かマスタか）を記録する。

【００４２】また、リーダ１において、ステップＳ６６で、トランスポンダ１８から送信されたシステム識別ＩＤが自身のものと一致しない場合、あるいは、ステップＳ７２で、トランスポンダ１８から送信されたマスタ・

キー・グループＩＤデータあるいは鍵ＩＤデータが自身のものと一致しない場合には、ステップＳ７８で、防犯および警報システムを作動させる。

【００４３】Ｂ－３．開錠処理（③ＣＰＵ無し、ＩＤ更新機能有り）

次に、ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り）１８を用いた場合における開錠処理について説明する。ここで、図１３および図１４は、ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り）１８における、リーダ１およびトランスポンダ１８での開錠処理の動作を説明するためのフローチャートである。

【００４４】まず、自動販売機のリーダ１では、図１３に示すステップＳ９０で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップＳ９２で、ＲＦパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップＳ９４でデータを受信するまで、所定時間間隔で、ＲＦパワー信号の送信を繰り返す。

【００４５】これに対して、鍵のトランスポンダ１８は、上記ＲＦパワー信号を受信することで作動し、図１４に示すステップＳ１１０で、ＥＥＰＲＯＭ２７からシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを読み込む。次に、ステップＳ１１２で、図７に示すデータフォーマットで、システム識別ＩＤデータマスタ・キー・グループＩＤデータおよび鍵ＩＤデータを送信する。

【００４６】リーダ１では、ステップＳ９４で、上記システム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを受信し、ステップＳ９６で、自身のＥＥＰＲＯＭ９に予め設定されているシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータと照合し、一致すれば、ステップＳ９８に進み、リレー１４を駆動し、電気錠２０を開く。そして、ステップＳ１００で、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を乱数によって生成し、ＥＥＰＲＯＭ９のＩＤデータを更新し、記憶する。次に、ステップＳ１０２で、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を送信する。

【００４７】これに対して、鍵のトランスポンダ１８では、ステップＳ１１４で、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を受信し、ステップＳ１１６で、該新たなＩＤデータで、ＥＥＰＲＯＭ２７のＩＤデータを書き換え、更新する。

【００４８】さらに、自動販売機のリーダ１では、ステップＳ１０４で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵）１８を識別するための鍵ＩＤデータ（個別かマスタか）を記録する。

【００４９】また、リーダ１において、ステップＳ９６で、トランスポンダ１８から送信されたシステム識別ＩＤ、マスタ・キー・グループＩＤデータまたは鍵ＩＤデータのいずれか１つでも自身のものと一致しない場合には、ステップＳ１０６で、防犯および警報システムを作動させる。

【００５０】Ｂ－４．開錠処理（④ＣＰＵ無し、ＩＤ更新機能無し）

次に、ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能無し）１８を用いた場合における開錠処理について説明する。ここで、図１５および図１６は、ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能無し）１８における、リーダ１およびトランスポンダ１８での開錠処理の動作を説明するためのフローチャートである。

【００５１】まず、自動販売機のリーダ１では、図１５に示すステップＳ１２０で、鍵穴に鍵が挿入されたか否かを判断し、鍵が挿入されると、ステップＳ１２２で、ＲＦパワー信号を送信する。なお、カード状の鍵を用いた場合には、後述するステップＳ１２４でデータを受信するまで、所定時間間隔で、ＲＦパワー信号の送信を繰り返す。

【００５２】これに対して、鍵のトランスポンダ１８は、上記ＲＦパワー信号を受信することで作動し、図１６に示すステップＳ１４０で、ＥＥＰＲＯＭ２７からシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを読み込む。次に、ステップＳ１４２で、図７に示すデータフォーマットで、システム識別ＩＤデータマスタ・キー・グループＩＤデータおよび鍵ＩＤデータを送信する。

【００５３】リーダ１では、ステップＳ１２４で、上記システム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータを受信し、ステップＳ１２６で、自身のＥＥＰＲＯＭ９に予め設定されているシステム識別ＩＤデータ、マスタ・キー・グループＩＤデータおよび鍵ＩＤデータと照合し、一致すれば、ステップＳ１２８に進み、リレー１４を駆動し、電気錠２０を開く。さらに、自動販売機のリーダ１では、ステップＳ１３０で、システム運用データとして、開錠した日時、開錠に用いられたトランスポンダ（鍵またはカード）１８を識別するための鍵ＩＤデータ（個別かマスタか）を記録する。

【００５４】また、リーダ１において、ステップＳ１２６で、トランスポンダ１８から送信されたシステム識別ＩＤ、マスタ・キー・グループＩＤデータまたは鍵ＩＤデータのいずれか１つでも自身のものと一致しない場合には、ステップＳ１３２で、防犯および警報システムを作動させる。

【００５５】Ｂ－５．ＩＤデータ設定処理（ＣＰＵ有り）

次に、ＣＰＵ２３を備えるトランスポンダ１８を用いた

場合におけるＩＤデータ設定処理について説明する。当該ＩＤデータ設定処理は、自動販売機の出荷時、鍵の紛失、盗難あるいは鍵穴の破壊などの場合に、リーダ１およびトランスポンダ１８に既に設定されているＩＤデータ（マスターキーグループＩＤデータまたは／および鍵ＩＤデータ）を変更する場合に実行される。ここで、図１７ないし図１９は、ＣＰＵ２３を備えるトランスポンダ（ＩＤ更新機能有り・無し）１８における、設定器（図示略）、リーダ１およびトランスポンダ１８におけるＩＤデータ設定処理の動作を説明するためのフローチャートである。

【００５６】図示しない設定器では、まず、ステップＳ１５０で、新ＩＤデータ（マスターキーグループＩＤデータまたは／および鍵ＩＤデータ）が設定され、リーダ１のデータ通信範囲内に移動させられる。そして、リーダ１のデータ通信範囲内に移動すると、ステップＳ１５２で、自動販売機のリーダ１に対してシステム識別ＩＤデータを送信する。

【００５７】これに対して、自動販売機のリーダ１では、設定器が該リーダの通信範囲内に移動した時点で、図１８に示すステップＳ１６０において、設定器から送信されるデータ（システム識別ＩＤ）を自動的に受信する。次に、データを受信すると、ステップＳ１６２で、受信したデータがＥＥＰＲＯＭ９に予め設定されているシステム識別ＩＤと一致するか照合し、一致すると、ステップＳ１６４に進み、設定器に対してマスタ・キー・グループＩＤデータ要求コマンドを送信する。

【００５８】設定器では、ステップＳ１５４で、リーダ１からマスタ・キー・グループＩＤデータ要求コマンドを受信すると、ステップＳ１５６で、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を設定するというコマンド、言い換えると、マスタ・キー・グループＩＤデータ要求コマンドに対するマスタ・キー・グループＩＤデータ以外の所定のデータを、自動販売機のリーダ１に対して送信した後、ステップＳ１５８で、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）をリーダ１に対して送信する。

【００５９】自動販売機のリーダ１では、ステップＳ１６６で、マスタ・キー・グループＩＤデータ要求に対するデータを受信し、ステップＳ１６８で、受信したデータが新たなＩＤデータの設定データ（コマンド）であるか判断し、設定データであると、ステップＳ１７０に進み、設定器から送信された新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を受信する。次に、ステップＳ１７２で、受信した新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）でＥＥＰＲＯＭ９に格納されているＩＤデータを更新し、記憶する。そして、ステップＳ１７４で、鍵のトランスポンダ１８に対して、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を送信する。

【００６０】これに対して、鍵のトランスポンダ１８では、当該トランスポンダ１８がリーダのデータ通信範囲にあると、図１９に示すステップＳ１９０で、新ＩＤデータを自動的に受信し、ステップＳ１９２で、受信した新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）でＥＥＰＲＯＭ２４に格納されているＩＤデータを更新し、記憶する。

【００６１】一方、リーダ１では、図１８に示すステップＳ１７６で、システムのＩＤデータ変更完了処理として、鍵のトランスポンダ１８との間でＩＤデータを授受することにより、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）の変更を確認する。そして、ステップＳ１７８で、システム運用データとして、ＩＤデータを変更（設定）した日時、トランスポンダ（鍵）１８を識別するための鍵ＩＤデータ（個別かマスタか）、およびＩＤデータを変更（設定）したことを記録する。

【００６２】また、自動販売機のリーダ１において、ステップＳ１６２で、設定器から送信されたシステム識別ＩＤと自身のシステム識別ＩＤとが一致しない場合、あるいは、ステップＳ１６８で、受信したデータが新たなＩＤデータの設定データ（コマンド）でない場合には、ステップＳ１８０で、防犯および警報システムを作動させる。

【００６３】このように、上述した処理によれば、ＣＰＵ２３を備えているトランスポンダ１８を用いる場合には、新たなＩＤデータを設定する際に、システムＩＤデータを自動販売機のリーダ１に送信するとともに、リーダ１からのマスタ・キー・グループＩＤデータ要求コマンドに対して所定のデータを送信することで、該リーダ１を自動的に新たなＩＤデータ受信処理へ移行させることができる。したがって、リーダ１およびトランスポンダ１８は、通常のデータ授受処理と同様のデータ授受処理を行うことで、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を設定することができる。

【００６４】Ｂ－６．ＩＤデータ設定処理（ＣＰＵ無し）

次に、ＣＰＵを備えていないトランスポンダ１８を用いた場合におけるＩＤデータ設定処理について説明する。ここで、図２０ないし図２１は、ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り・無し）１８における、設定器（図示略）、リーダ１およびトランスポンダ１８におけるＩＤデータ設定処理の動作を説明するためのフローチャートである。

【００６５】図示しない設定器では、まず、図２０に示すステップＳ２００で、新ＩＤデータ（マスターキーグループＩＤデータまたは／および鍵ＩＤデータ）が設定

され、リーダ１のデータ通信範囲内に移動させられる。そして、リーダ１のデータ通信範囲内に移動すると、ステップＳ２０２で、自動販売機のリーダ１に対して、設定器を識別するための設定器ＩＤデータを送信した後、ステップＳ２０４で、新たなＩＤデータを送信する。

【００６６】これに対して、自動販売機のリーダ１では、設定器が通信範囲内に移動した時点で、図２１に示すステップＳ２１０において、設定器から送信される設定器ＩＤデータを自動的に受信する。次に、設定器ＩＤデータを受信すると、ステップＳ２１２で、受信した設定器ＩＤデータが所定のデータであるか照合し、所定のデータである場合には、ステップＳ２１４に進み、設定器から送信される新たなＩＤデータを受信する。

【００６７】次に、リーダ１は、ステップＳ２１６で、受信した新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）でＥＥＰＲＯＭ９に格納されているＩＤデータを更新し、記憶する。そして、ステップＳ２１８で、鍵のトランスポンダ１８に対して、上記新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を送信する。

【００６８】これに対して、鍵のトランスポンダ１８では、当該トランスポンダ１８がリーダ１のデータ通信範囲にあると、図２２に示すステップＳ２３０で、新ＩＤデータを自動的に受信し、ステップＳ２３２で、受信した新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）でＥＥＰＲＯＭ２７に格納されているＩＤデータを更新し、記憶する。

【００６９】一方、リーダ１では、図２１に示すステップＳ２２０で、システムのＩＤデータ変更完了処理として、鍵のトランスポンダ１８との間でＩＤデータを授受することにより、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）の変更を確認する。そして、ステップＳ２２２で、システム運用データとして、ＩＤデータを変更（設定）した日時、トランスポンダ（鍵）１８を識別するための鍵ＩＤデータ（個別かマスタか）およびＩＤデータを変更（設定）したことを記録する。

【００７０】また、自動販売機のリーダ１において、ステップＳ２１２で、設定器から送信された設定器ＩＤデータが所定のデータでない場合には、ステップＳ２２４で、防犯および警報システムを作動させる。

【００７１】このように、上述した処理によれば、ＣＰＵ２３を備えていないトランスポンダ１８を用いる場合、新たなＩＤデータを設定する際に、設定器固有の設定器ＩＤデータを自動販売機のリーダ１に送信することで、該リーダ１を自動的に新たなＩＤデータ受信処理へ移行させることができる。したがって、リーダ１およびトランスポンダ１８は、通常のデータ授受処理と同様のデータ授受処理を行うことで、新たなＩＤデータ（マスタ・キー・グループＩＤデータまたは／および鍵ＩＤデータ）を設定することができる。

【００７２】なお、上記実施例では、鍵のトランスポンダと自動販売機のリーダとのＩＤデータが不一致である場合、防犯および警報システムを作動させるようにしたが、具体的には、警報音を鳴らしたり、防犯カメラを作動させたり、通信回線を介して通報したりというように、少なくとも１つ、あるいはこれらを組み合わせて用いる。

【００７３】

【発明の効果】請求項１記載の発明によれば、応答装置が自動販売機に近接すると、読み取り装置の高周波発生手段からの高周波磁界を電力とし、第１の送信手段から第１の記憶手段に記憶されている応答装置識別データが送信され、該応答装置識別データが読み取り装置の第２の記憶手段に記憶されている応答装置識別データとが一致すると、電気錠が開錠されるようにしたので、外部から錠の位置が分からず、錠の破壊を防止することができるという利点が得られる。

【００７４】また、請求項２記載の発明によれば、前記第１受信手段によって受信された応答装置識別データと前記第２の記憶手段に記憶されている応答装置識別データとが一致しない場合、警告手段によって警告を発するようにしたので、不正な応答装置または不正な鍵による開錠、もしくは錠の破壊を防止することができるという利点が得られる。

【００７５】また、請求項３記載の発明によれば、前記応答装置を鍵形状部分とし、前記自動販売機の前記電気錠が設けられる位置とは異なる位置に、前記応答装置の鍵形状部分が挿入される鍵穴部を備え、前記読み取り装置は、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことを検知する検出手段を備えるようにしたので、仮に錠穴が破壊されても、電気錠でロックされてますので、扉を開けることはできず、盗難を防止することができ、かつ、電気錠自体が破壊されることは避けられるので、被害規模を最小にすることができるという利点が得られる。

【００７６】また、請求項４記載の発明によれば、前記読み取り装置の前記検出手段によって、前記鍵穴部に前記応答装置の鍵形状部分が挿入されたことが検知された時点で、前記高周波発生手段によって高周波磁界を発生するようにしたので、電力消費を低減することができるという利点が得られる。

【００７７】また、請求項５記載の発明によれば、前記応答装置をカード形状とし、前記読み取り装置の前記高周波発生手段によって所定時間間隔で前記高周波磁界を発生するようにしたので、自動販売機に鍵穴を設ける必要がなく、錠の破壊を防止することができるという利点が得られる。

【００７８】また、請求項６記載の発明によれば、前記

応答装置および前記読み取り装置は、前記応答装置識別データに加えて、システムを識別するシステム識別データおよび自動販売機の設置地域を識別するマスタ・キー・グループ識別データを授受するようにしたので、より安全性を向上させることができるという利点が得られる。

【００７９】また、請求項７記載の発明によれば、前記応答装置に、所定の通信プロトコルに従って、前記読み取り装置との間におけるデータ授受を制御する第２の制御手段を備え、前記応答装置および前記読み取り装置との間で、前記所定の通信プロトコルに従って、前記システム識別データ、前記マスタ・キー・グループ識別データおよび前記応答装置識別データを授受するようにしたので、より機密性を向上させることができ、より安全性を向上させることができるという利点が得られる。

【００８０】また、請求項８記載の発明によれば、電気錠を開錠する度に、認証に必要な応答装置識別データを書き換えるようにしたので、より機密性を向上させることができ、より安全性を向上させることができるとともに、応答装置の不正なコピーを防止できるという利点が得られる。

【００８１】また、請求項９記載の発明によれば、前記応答装置識別データおよびマスタ・キー・グループ識別データを外部設定装置により無線通信により書換可能とするようにしたので、応答装置（鍵）の紛失、盗難あるいは鍵穴の破壊が生じた場合でも、非接触で識別データの書き換えができるので、ハードウェアを取り替えることなく、更新できるという利点が得られる。

【図面の簡単な説明】

【図１】本発明の実施例による自動販売機システムの構成を示すブロック図である。

【図２】トランスポンダがカード形状の場合におけるリーダが内蔵された自動販売機の外観構成を示す斜視図である。

【図３】トランスポンダが鍵状の場合におけるリーダが内蔵された自動販売機の外観構成を示す斜視図である。

【図４】トランスポンダのより詳細な構成例を示すブロック図である。

【図５】トランスポンダがＣＰＵを備える場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図６】トランスポンダがＣＰＵを備える場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図７】トランスポンダがＣＰＵを備えない場合におけるリーダとトランスポンダとで授受されるデータフォーマットを示す概念図である。

【図８】トランスポンダがＣＰＵを備えない場合におけるリーダとトランスポンダとの間でのデータ授受を示す概念図である。

【図９】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能有り）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図１０】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能有り）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図１１】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能無し）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図１２】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能無し）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図１３】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図１４】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図１５】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能無し）の場合における、リーダでの開錠処理の動作を説明するためのフローチャートである。

【図１６】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能無し）の場合における、トランスポンダでの開錠処理の動作を説明するためのフローチャートである。

【図１７】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能有り・無し）の場合における、設定器（図示略）でのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【図１８】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能有り・無し）の場合、リーダでのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【図１９】ＣＰＵを備えるトランスポンダ（ＩＤ更新機能有り・無し）の場合における、トランスポンダでのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【図２０】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り・無し）の場合における、設定器（図示略）でのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【図２１】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り・無し）の場合、リーダでのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【図２２】ＣＰＵを備えていないトランスポンダ（ＩＤ更新機能有り・無し）の場合における、トランスポンダでのＩＤデータ設定処理の動作を説明するためのフローチャートである。

【符号の説明】

１　リーダ

２　変調回路（高周波発生手段、第２の送信手段）

３　ＲＦパワー送信機（高周波発生手段、第２の送信手

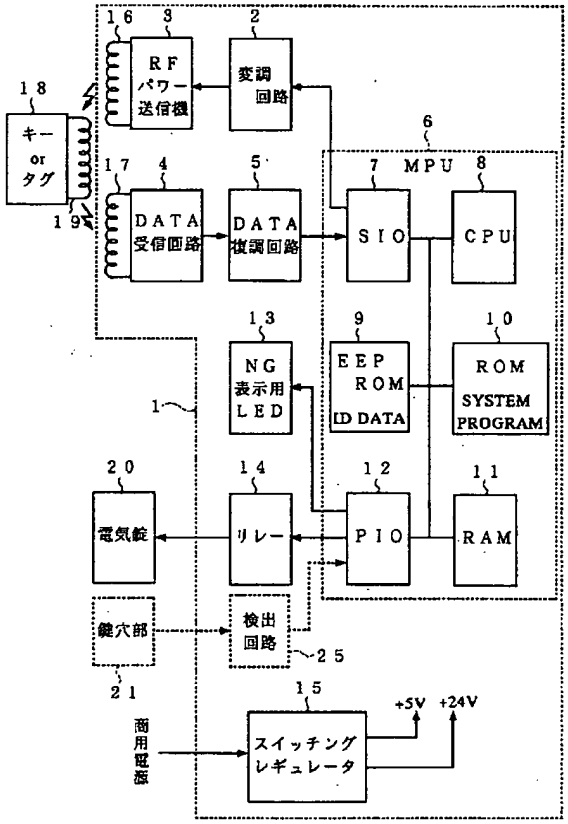
19

段）
４　ＤＡＴＡ受信回路（第１の受信手段）
５　ＤＡＴＡ復調回路（第１の受信手段）
６　ＭＰＵ
７　ＳＩＯ
８　ＣＰＵ（第１の制御手段、応答装置識別データ生成手段、第１の更新手段）
９　ＥＥＰＲＯＭ（第２の記憶手段）
１０　ＲＯＭ
１１　ＲＡＭ
１２　ＰＩＯ
１３　ＮＧ表示用ＬＥＤ（警告手段）
１４　リレー（第１の制御手段）
１５　スイッチングレギュレータ

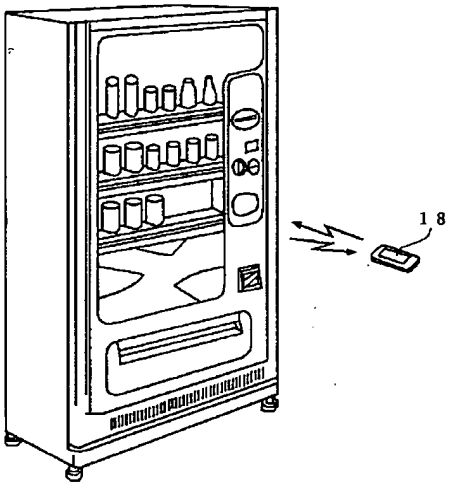
20

＊１６，１７　アンテナ
１８　トランスポンダ
１９　アンテナ
２０　電気錠
２１　鍵穴
２２　送受信回路（第１の送信手段、第２の受信手段、第２の更新手段）
２３　ＣＰＵ（第２の制御手段）
２４　ＥＥＰＲＯＭ（第１の記憶手段）
２５　検出回路（検出手段）
２６　送受信回路（第１の送信手段、第２の受信手段、第２の更新手段）
２７　ＥＥＰＲＯＭ（第１の記憶手段）

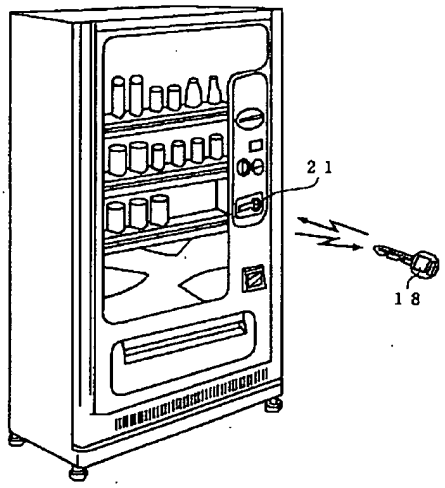
【図１】



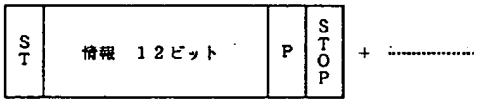
【図２】



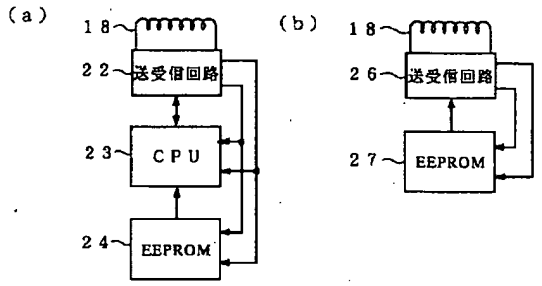
【図３】



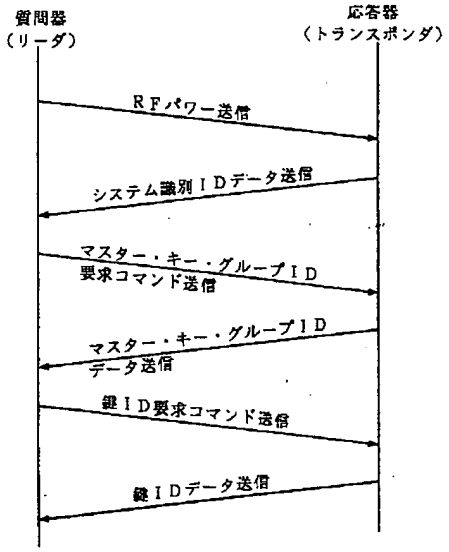
【図５】



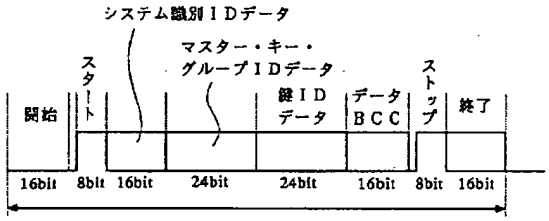
【図4】



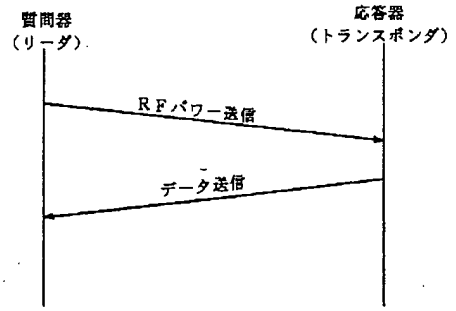
【図6】



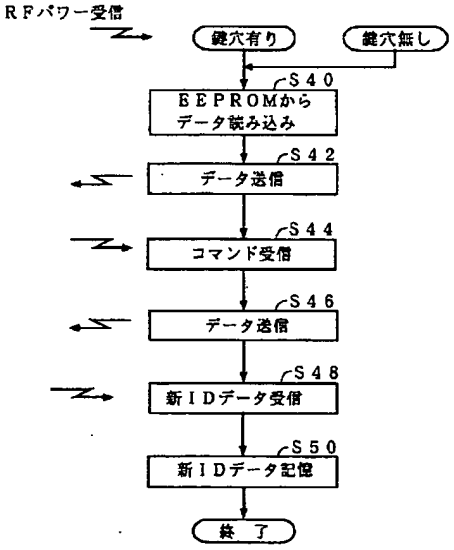
【図7】



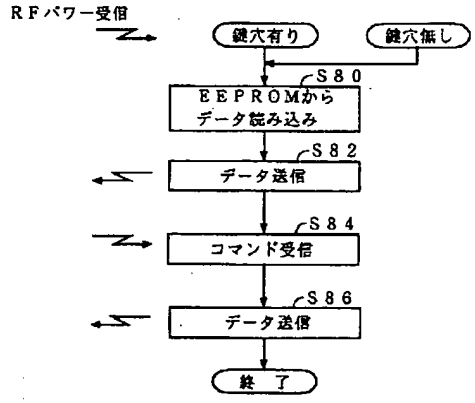
【図8】



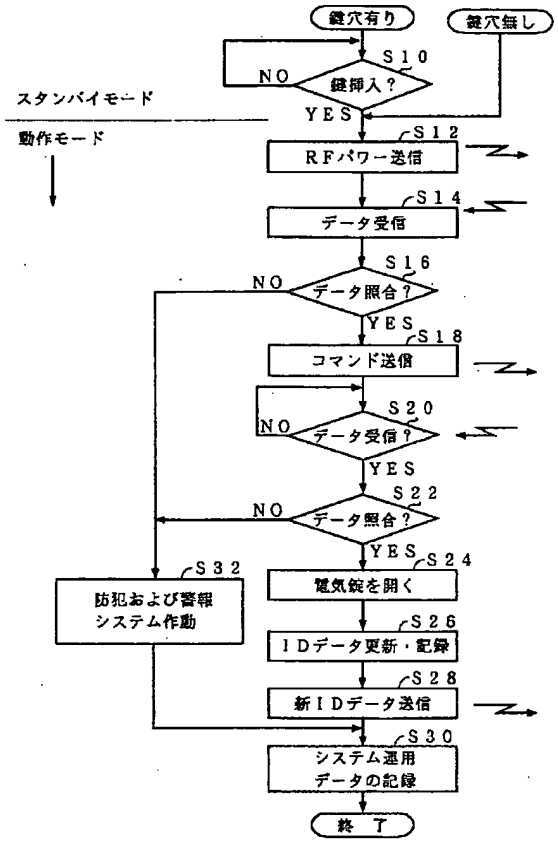
【図10】



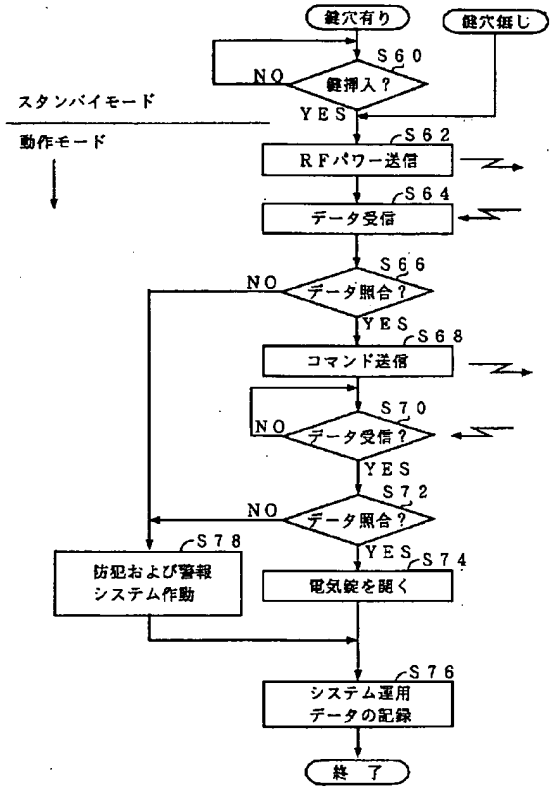
【図12】



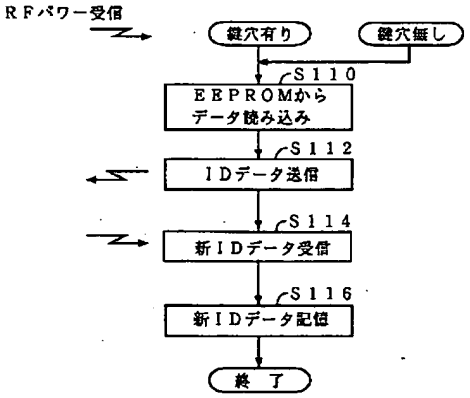
【図9】



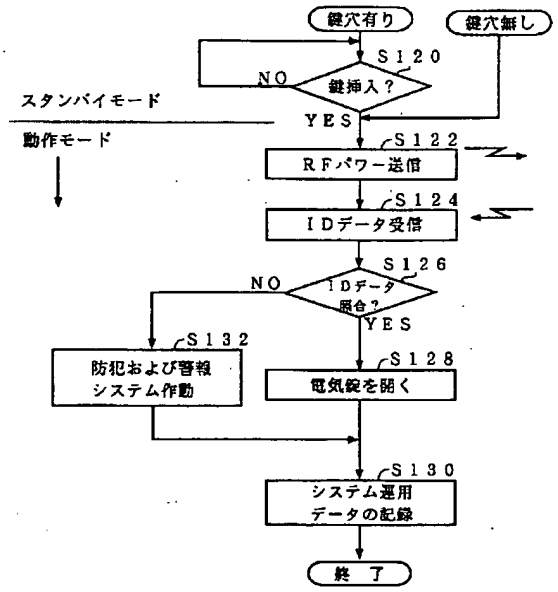
【図11】



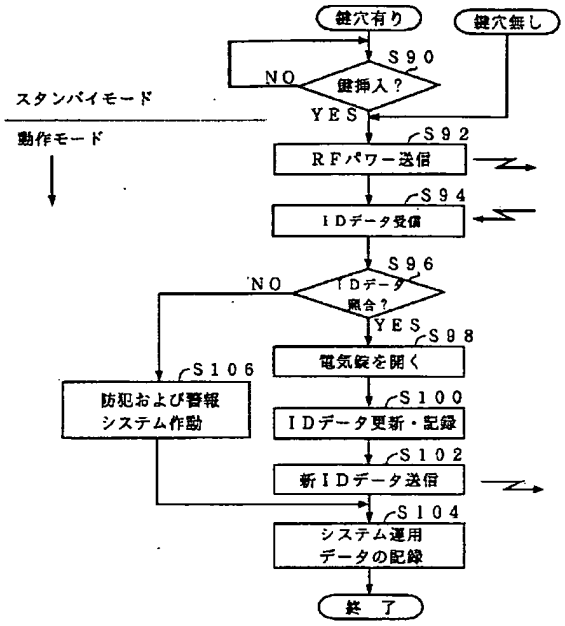
【図14】



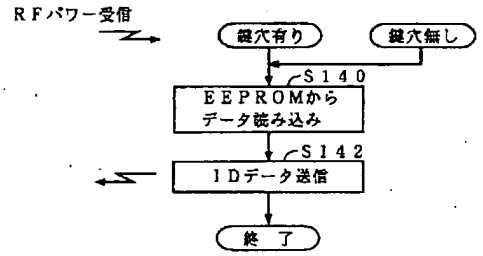
【図15】



【図１３】

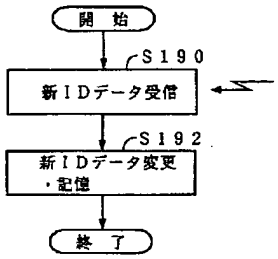


【図１６】

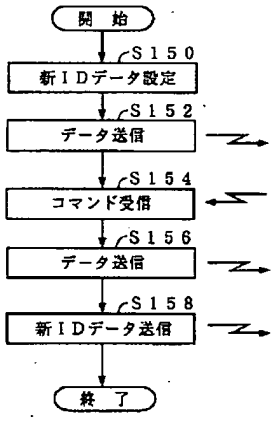


【図１９】

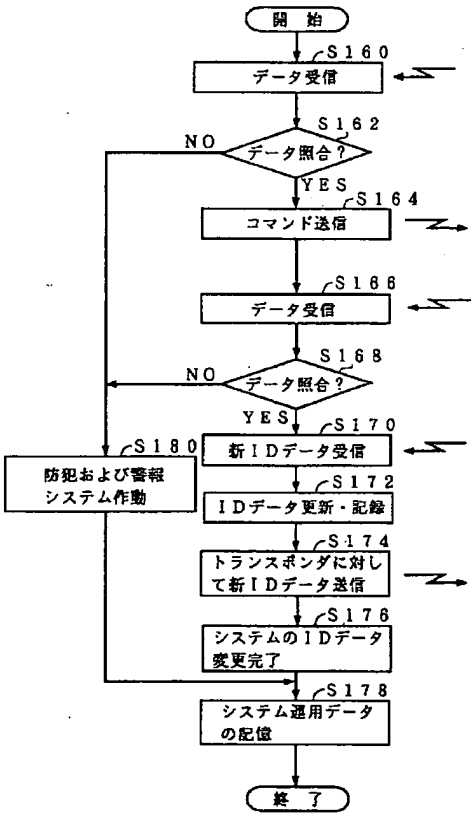
IDデータ設定時のトランスポンダ



【図１７】

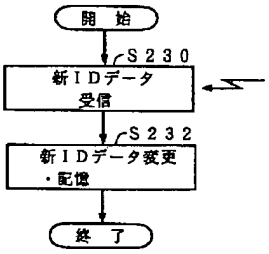


【図１８】

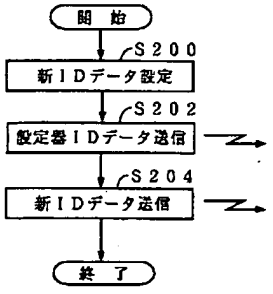


【図２２】

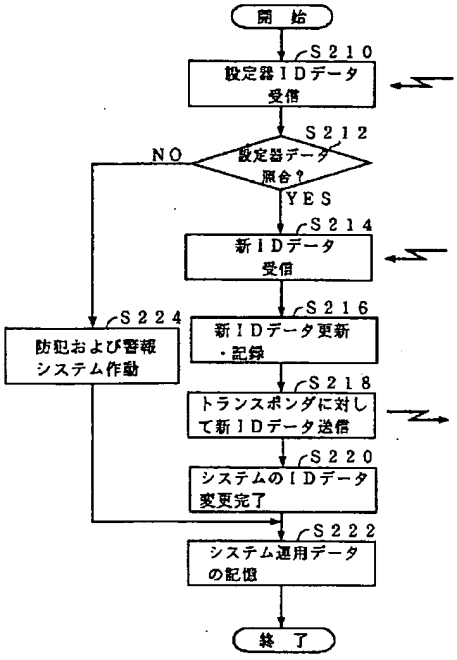
IDデータ設定時のトランスポンダ



【図２０】



【図21】


開 始
S210
設定器IDデータ受信
S212
設定器データ照合？
NO
YES
S214
新IDデータ受信
S216
新IDデータ更新・記録
S218
トランスポンダに対して新IDデータ送信
S220
システムのIDデータ変更完了
S224
防犯および警報システム作動
S222
システム運用データの記憶
終 了